

Sai Vegasena

Website: svegas18.me Email: sv232@nyu.edu Github: github.com/sv232

Experience

Security Engineering Intern at Trail of Bits 6/18 - Present

Integrated just in time LLVM lifting with remill allowing klee instrumentation/symbolic execution on x86 machine code

Security Intern at MWR Infosecurity an F-Secure Company 5/18 - 8/18

Conducted application and network assessments on client code and published a blog-post on coverage guided fuzzing.

OSIRIS Lab Researcher\NYUSEC CTF Team Member 12/16 - Present

Participate in the cybersecurity research lab and NYU CTF Team. Currently help run CSAW, HSF/CSAW RED.

CSAW 2017/2018: Organizer and Problem Writer **HSF 2017:** Problem Writer **CSAW RED 2018:** Problem Writer

Projects

trailofbits/klee 7/18 - 8/18

Adding syscall emulation and a custom runtime for remill lifted functions to klee's symbolic execution engine

osiris/vasilisk 7/18 - 8/18

Independent study with Brendan Dolan Gavitt for fuzzing v8 with grammar and mutation based techniques

Kleenex 7/18 - 8/18

C++ wrapper around KLEE and AFL for intelligent, coverage guided fuzzing. Developed for research at MWR.

Insanity 4/18 - 8/18

LLVM pass that obfuscates against symbolic execution

Horus 1/25 - Current

Pluggable framework that queries and puts "the internet" into a gigantic DB; finds dangling domains and publicly facing docker registries. Bug Bounties on 2 Alexa top 1000 domains and reported bounties to 15 large corporations.

PiBrain Assistant 11/17 - 1/18

Seq2Seq implementation using tensorflow and neural machine translation to build a cost effective assistant

Technologies/Skills

Binary Exploitation: Binaryninja, KLEE, AFL, IDA, Angr, Pwntools, Pwndbg, GDB, Manticore, Apktool, Windbg

Web: Burp Suite, Kali Linux, Nessus, Metasploit, SQLmap, Heroku, Flask, MySQL/SQLAlchemy, Jekyll, Git

ML: Tensorflow, Openai API **Infra:** Docker **Creative:** Processing, Particles.js

Education

New York University; B.S in Computer Science 2016 - 2020 (expected)

Languages

C C++ Python LLVM Rust Go Bash HTML SQL CSS JavaScript x86 MIPS